ABSTRACT OF THE DISCLOSURE

A method and apparatus is provided for securely executing access control functions that may be customized by or on behalf of administrators of information access systems. Examples of such functions include changing a password of a user, determining whether or not data specifying a user and a password identifies an authentic user, and displaying a message indicating whether a login attempt was successful. An access control function is mapped to a digital signature. The digital signature is used to verify that an executable element retrieved for executing the access control function is the proper executable element. The access control functions may be invoked upon the occurrence of access control events, such as a user successfully logging onto an information access system or the modification of a user's password. A mapping contains data used to determine what events are tied to what access control functions, and whether the access control function should be executed. Upon the occurrence of an extension event that is tied to an extension, an executable element for the extension is retrieved. After executing an extension, data is returned to the caller of the extension. The returned data may be a hash table that includes other objects, such as strings or even other hash tables. The access control functions are developed in manner that exploits the power and simplicity of the inheritance feature of object oriented programming.